CLAIMS

1. An information recorder for recording information to a recording medium, the apparatus comprising:

a cryptography means for encrypting information to be recorded to the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation; and

a user interface for making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of the information recorder and prerecording generation information which is recording-medium generation information prestored in the recording medium, and outputting a warning when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

2. The apparatus according to claim 1, wherein the device-stored generation-managed encryption key is a master key stored in common to a plurality of information recorders.

3. The apparatus according to claim 1, wherein the cryptography means includes means for renewing, when the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key, a generation-managed encryption key of a generation as young as or younger than

that indicated by the prerecording generation information.

4. The apparatus according to claim 1, wherein the cryptography means includes means for creating, based on the device-stored generation-managed encryption key, a generation-managed encryption key whose generation information is older than the generation information on the device-stored generation-managed encryption key.

5. The apparatus according to claim 1, wherein:

the cryptography means includes means for renewing, when the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key, a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information; and

the key renewing means decrypts an encrypted to-be-renewed generation-managed encryption key with a device key stored in the information recorder to create an renewed generation-managed encryption key.

6. The apparatus according to claim 5, wherein the cryptography means acquires a key table in which the encrypted to-be-renewed generation-managed encryption key and a decrypting device key identifier are correlated with each other to decrypt the encrypted to-be-renewed generation-managed encryption key with a device key identified based on the device key identifier in the key table.

7. The apparatus according to claim 5, wherein the device key is a key common to information recorders grouped by categorization into a common category.

8. The apparatus according to claim 5, wherein the device key is a key common to information recorders enclosed in the same group by grouping based on serial numbers assigned to the information recorders.

9. The apparatus according to claim 1, wherein:

there are held a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information recorders each as a leaf and a leaf key unique to each of the information recorders; and

the generation-managed encryption key is a key which can be renewed with at least either the node key or leaf key.

10. The apparatus according to claim 9, wherein the generation-managed encryption key is a master key common to the plurality of information recorders.

11. The apparatus according to claim 9, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the node key has to be renewed; and

the cryptography means in the information recorder receives renewal data for the generation-managed encryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-managed encryption key based on the thus-acquired renewed

node key.

12. The apparatus according to claim 9, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

13. The apparatus according to claim 9, wherein:

the generation-managed encryption key has a generation number as renewal information correlated therewith; and

the cryptography means stores, as a recording generation number into the recording medium, a generation number of the generation-managed encryption key having been used for storing encrypted data into the recording medium.

14. An information recorder for recording information to a recording medium, the apparatus comprising:

a cryptography means for encrypting information to be recorded to the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation; and

a key acquiring means for making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of the information recorder and prerecording generation information which is recording-medium generation information prestored in the recording medium, and acquiring a generation-managed encryption key of a generation as young as or younger than that

indicated by the prerecording generation information when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

15. The apparatus according to claim 14, wherein the key acquiring means includes a communication interface capable of receiving data via a network.

16. The apparatus according to claim 14, wherein the key acquiring means includes a communication modem capable of receiving data via a telephone line.

17. The apparatus according to claim 14, wherein the key acquiring means includes an I/C card interface capable of receiving data via an IC card.

18. The apparatus according to claim 14, wherein:

the cryptography means makes a mutual authentication with a key serving means when the key acquiring means is going to acquire the generation-managed encryption key; and

the key acquiring means effects the acquisition of the generation-managed key only when the mutual authentication with the key serving means has successfully been made.

19. The apparatus according to claim 14, wherein the device-stored generation-managed encryption key is a master key common to a plurality of information recorders.

20. The apparatus according to claim 14, wherein the cryptography means includes means for renewing, when the prerecording generation information is newer

than the generation information on the device-stored generation-managed encryption key, a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information.

21. The apparatus according to claim 14, wherein the cryptography means includes a key creating means for creating, based on the device-stored generation-managed encryption key, a generation-managed encryption key whose generation information is older than the generation information on the device-stored generation-managed encryption key.

22. The apparatus according to claim 14, wherein:

the cryptography means includes means for renewing, when the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key, a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information; and

the key renewing means decrypts an encrypted to-be-renewed generation-managed encryption key with a device key stored in the information recorder to create an renewed generation-managed encryption key.

23. The apparatus according to claim 22, wherein the cryptography means acquires a key table in which the encrypted to-be-renewed generation-managed encryption key and a decrypting device key identifier are correlated with each other to decrypt the encrypted to-be-renewed generation-managed encryption key with a device

key identified based on the device key identifier in the key table.

24. The apparatus according to claim 22, wherein the device key is a key common to information recorders grouped by categorization into a common category.

25. The apparatus according to claim 22, wherein the device key is a key common to information recorders enclosed in the same group by grouping based on serial numbers assigned to the information recorders.

26. The apparatus according to claim 14, wherein:

there are held a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information recorders each as a leaf and a leaf key unique to each of the information recorders; and

the generation-managed encryption key is a key which can be renewed with at least either the node key or leaf key.

27. The apparatus according to claim 26, wherein the generation-managed encryption key is a master key common to the plurality of information recorders.

28. The apparatus according to claim 26, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the node key has to be renewed; and

the cryptography means in the information recorder receives renewal data for

the generation-managed encryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-managed encryption key based on the thus-acquired renewed node key.

29. The apparatus according to claim 26, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

30. The apparatus according to claim 26, wherein:

the generation-managed encryption key has a generation number as renewal information correlated therewith; and

the cryptography means stores, as a recording generation number into the recording medium, a generation number of the generation-managed encryption key having been used for storing encrypted data into the recording medium.

31. An information recorder for recording information to a recording medium, the apparatus comprising:

a cryptography means for encrypting information to be recorded to the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation; and

a key renewing terminal connecting interface for connection of a key renewing terminal which makes a comparison between generation information on a device-stored

generation-managed encryption key stored in a storage means of the information recorder and prerecording generation information which is recording-medium generation information prestored in the recording medium, and acquires a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

32. The apparatus according to claim 31, wherein:

a mutual authentication with the key renewing terminal is effected to acquire the generation-managed encryption key from the key renewing terminal; and

the acquisition of the generation-managed encryption key is effected only when the mutual authentication with the key renewing terminal has successfully been made.

33. The apparatus according to claim 31, wherein:

there are held a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information recorders each as a leaf and a leaf key unique to each of the information recorders; and

the generation-managed encryption key is a key which can be renewed with at least either the node key or leaf key.

34. The apparatus according to claim 33, wherein the generation-managed encryption key is a master key common to the plurality of information recorders.

35. The apparatus according to claim 33, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the node key has to be renewed; and

the cryptography means in the information recorder receives renewal data for the generation-managed encryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-managed encryption key based on the thus-acquired renewed node key.

36. The apparatus according to claim 33, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

37. The apparatus according to claim 33, wherein :

the generation-managed encryption key has a generation number as renewal information correlated therewith; and

the cryptography means stores, as a recording generation number into the recording medium, a generation number of the generation-managed encryption key having been used for storing encrypted data into the recording medium.

38. An information player for playing back information from a recording

medium, the apparatus comprising:

a cryptography means for decrypting information read from the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation; and

a user interface for making a comparison between generation information on a device-stored generation-managed decryption key stored in a storage means of the information player and recording generation information which is generation information having been used for recording the information to the recording medium, and outputting a warning when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

39. The apparatus according to claim 38, wherein the cryptography means does not make any information decryption when a comparison made between the recording generation information which is generation information having been used for recording the information to the recording medium and prerecording generation information which is recording medium generation information prestored in the recording medium shows that the prerecording generation information is newer than the recording generation information.

40. The apparatus according to claim 38, wherein the device-stored generation-managed decryption key is a master key stored in common to a plurality of information players.

41. The apparatus according to claim 38, wherein the cryptography means includes means for renewing, when the prerecording generation information is newer than the generation information on the device-stored generation-managed decryption key, a generation-managed decryption key of a generation as young as or younger than that indicated by the prerecording generation information.

42. The apparatus according to claim 38, wherein the cryptography means includes a key creating means for creating, based on the device-stored generation-managed decryption key, a generation-managed decryption key whose generation information is older than the generation information on the device-stored generation-managed decryption key.

43. The apparatus according to claim 38, wherein the cryptography means includes means for renewing, when the recording generation information is newer than the generation information on the device-stored generation-managed encryption key, a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information; and

the key renewing means decrypts an encrypted to-be-renewed generation-managed encryption key with a device key stored in the information player to create an renewed generation-managed encryption key.

44. The apparatus according to claim 43, wherein the cryptography means acquires a key table in which the encrypted to-be-renewed generation-managed encryption key and a decrypting device key identifier are correlated with each other to

decrypt the encrypted to-be-renewed generation-managed encryption key with a device key identified based on the device key identifier in the key table.

45. The apparatus according to claim 43, wherein the device key is a key common to information players grouped by categorization into a common category.

46. The apparatus according to claim 43, wherein the device key is a key common to information players enclosed in the same group by grouping based on serial numbers assigned to the information players.

47. The apparatus according to claim 38, wherein:

there are held a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information players each as a leaf and a leaf key unique to each of the information players; and

the generation-managed encryption key is a key which can be renewed with at least either the node key or leaf key.

48. The apparatus according to claim 47, wherein the generation-managed encryption key is a master key common to the plurality of information players.

49. The apparatus according to claim 47, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the node key has to be renewed; and

the cryptography means in the information player receives renewal data for the generation-managed decryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-managed decryption key based on the thus-acquired renewed node key.

50. The apparatus according to claim 47, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

51. The apparatus according to claim 47, wherein:

the generation-managed decryption key has a generation number as renewal information correlated therewith; and

for decryption of encrypted data read from the recording medium, the cryptography means reads, from the recording medium, a generation number of the generation-managed encryption key having been used for encrypting the data and decrypts the encrypted data with a generation-managed decryption key corresponding to the thus-read generation number.

52. An information player for playing back information from a recording medium, the apparatus comprising:

a cryptography means for decrypting information read from the recording medium by a cryptography with a generation-managed decryption key which is

renewed to a different key for each generation; and

a key acquiring means for making a comparison between generation information on a device-stored generation-managed decryption key stored in a storage means of the information player and recording generation information which is generation information having been used for recording the information, and acquiring a generation-managed decryption key of a generation as young as or younger than that indicated by the recording generation information when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

53. The apparatus according to claim 52, wherein the cryptography means does not make any information decryption when a comparison made between the recording generation information which is generation information having been used for recording the information to the recording medium and prerecording generation information which is recording medium generation information prestored in the recording medium shows that the prerecording generation information is newer than the recording generation information.

54. The apparatus according to claim 52, wherein the key acquiring means includes a communication interface capable of receiving data via a network.

55. The apparatus according to claim 52, wherein the key acquiring means includes a communication modem capable of receiving data via a telephone line.

56. The apparatus according to claim 52, wherein the key acquiring means

includes an I/C card interface capable of receiving data via an IC card.

57. The apparatus according to claim 52, wherein:

the cryptography means makes a mutual authentication with a key serving means when the key acquiring means is going to acquire the generation-managed decryption key; and

the key acquiring means effects the acquisition of the generation-managed key only when the mutual authentication with the key serving means has successfully been made.

58. The apparatus according to claim 52, wherein the device-stored generation-managed decryption key is a master key common to a plurality of information players.

59. The apparatus according to claim 52, wherein the cryptography means includes means for renewing, when the recording generation information is newer than the generation information on the device-stored generation-managed decryption key, a generation-managed decryption key of a generation as young as or younger than that indicated by the recording generation information.

60. The apparatus according to claim 52, wherein the cryptography means includes a key creating means for creating, based on the device-stored generation-managed encryption key, a generation-managed decryption key whose generation information is older than the generation information on the device-stored generation-managed decryption key.

61. The apparatus according to claim 52, wherein:

the cryptography means includes means for renewing, when the recording generation information is newer than the generation information on the device-stored generation-managed decryption key, a generation-managed encryption key of a generation as young as or younger than that indicated by the recording generation information; and

the key renewing means decrypts an encrypted to-be-renewed generation-managed decryption key with a device key stored in the information player to create an renewed generation-managed encryption key.

62. The apparatus according to claim 61, wherein the cryptography means acquires a key table in which the encrypted to-be-renewed generation-managed encryption key and a decrypting device key identifier are correlated with each other to decrypt the encrypted to-be-renewed generation-managed encryption key with a device key identified based on the device key identifier in the key table.

63. The apparatus according to claim 61, wherein the device key is a key common to information players grouped by categorization into a common category.

64. The apparatus according to claim 61, wherein the device key is a key common to information players enclosed in the same group by grouping based on serial numbers assigned to the information players.

65. The apparatus according to claim 52, wherein:

there are provided a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information players each as a leaf and

a leaf key unique to each of the information players; and

the generation-managed decryption key is a key which can be renewed with at least either the node key or leaf key.

66. The apparatus according to claim 65, wherein the generation-managed decryption key is a master key common to the plurality of information players.

67. The apparatus according to claim 65, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from decryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the node key has to be renewed; and

the cryptography means in the information player receives renewal data for the generation-managed decryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-managed decryption key based on the thus-acquired renewed node key.

68. The apparatus according to claim 65, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

69. The apparatus according to claim 65, wherein:

the generation-managed decryption key has a generation number as renewal information correlated therewith; and

for decryption of encrypted data read from the recording medium, the cryptography means reads, from the recording medium, a generation number of the generation-managed encryption key having been used for encrypting the data and decrypts the encrypted data with a generation-managed decryption key corresponding to the thus-read generation number.

70. An information player for playing back information from a recording medium, the apparatus comprising:

a cryptography means for decrypting information read from the recording medium by a cryptography with a generation-managed decryption key which is renewed to a different key for each generation; and

a key renewing terminal connecting interface for connection of a key renewing terminal which makes a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of the information player and recording generation information which is generation information having been used for recording the information to the recording medium and acquires a generation-managed decryption key of a generation as young as or younger than that indicated by the generation information on the device-stored generation-managed decryption key when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

71. The apparatus according to claim 70, wherein:

a mutual authentication with a key serving means is effected when the key acquiring means is going to acquire the generation-managed decryption key; and the

acquisition of the generation-managed key is effected only when the mutual authentication with the key serving means has successfully been made.

72. The apparatus according to claim 70, wherein:

there are held a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information players each as a leaf and a leaf key unique to each of the information players; and

the generation-managed decryption key is a key which can be renewed with at least either the node key or leaf key.

73. The apparatus according to claim 72, wherein the generation-managed decryption key is a master key common to the plurality of information players.

74. The apparatus according to claim 72, wherein the node key can be renewed,

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from decryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the node key has to be renewed; and

the cryptography means receives renewal data for the generation-managed decryption key encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and acquires renewal data for the generation-

managed decryption key based on the thus-acquired renewed node key.

75. The apparatus according to claim 72, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

76. The apparatus according to claim 72, wherein:

the generation-managed decryption key has a generation number as renewal information correlated therewith; and

for decryption of encrypted data read from the recording medium, the cryptography means reads, from the recording medium, a generation number of the generation-managed encryption key having been used for encrypting the data and decrypts the encrypted data with a generation-managed decryption key corresponding to the thus-read generation number.

77. An information recording method for recording information to a recording medium, the method comprising the steps of:

encrypting information to be recorded to the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation;

making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of an information recorder and prerecording generation information which is recording-medium

generation information prestored in the recording medium; and

outputting a warning when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

78. An information recording method for recording information to a recording medium, the method comprising the steps of:

encrypting information to be recorded to the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation; and

making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of the information recorder and prerecording generation information which is recording-medium generation information prestored in the recording medium; and

acquiring a generation-managed encryption key of a generation as young as or younger than that indicated by the prerecording generation information when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

79. The method according to claim 78, wherein the key acquiring step further includes the steps of:

renewing the generation-managed encryption key with at least either a node key unique to each of nodes included in a hierarchical tree structure including a plurality

of different information recorders each as a leaf or a leaf key unique to each of the information recorders; and

encrypting data to be recorded into the recording medium with the generation-managed encryption key renewed in the renewing step.

80. The method according to claim 79, wherein the generation-managed encryption key is a master key common to the plurality of information recorders.

81. The method according to claim 79, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the node key has to be renewed; and

the renewing step further including the steps of:

acquiring a renewed node key by encryption of the key renewal block (KRB); and

calculating renewal data for the generation-managed encryption key based on the thus-acquired renewed node key.

82. The method according to claim 79, wherein:

the generation-managed encryption key has a generation number as renewal information correlated therewith; and

the encrypting step further includes the step of:

storing, as a recording generation number into the recording medium, a generation number of the generation-managed encryption key having been used for storing encrypted data into the recording medium.

83. An information playback method for playing back information from a recording medium, the method including the steps of:

decrypting information read from the recording medium by a cryptography with a generation-managed encryption key which is renewed to a different key for each generation;

making a comparison between generation information on a device-stored generation-managed decryption key stored in a storage means of the information player and recording generation information which is generation information having been used for recording the information to the recording medium; and

outputting a warning when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

84. An information playback method for playing back information from a recording medium, the method including:

decrypting information read from the recording medium by a cryptography with a generation-managed decryption key which is renewed to a different key for each generation;

making a comparison between generation information on a device-stored

generation-managed decryption key stored in a storage means of an information recorder/player and recording generation information which is generation information having been used for recording the information; and

acquiring a generation-managed decryption key of a generation as young as or younger than that indicated by the recording generation information when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

85. The method according to claim 84, wherein the key acquiring step further includes the steps of:

renewing the generation-managed decryption key with at least either a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information players each as a leaf or a leaf key unique to each of the information players; and

decrypting data to be recorded into the recording medium with the generation-managed decryption key renewed in the renewing step.

86. The method according to claim 85, wherein the generation-managed decryption key is a master key common to the plurality of information players.

87. The method according to claim 85, wherein:

the node key can be renewed;

there is distributed, when a node key is to be renewed, a key renewal block (KRB) derived from encryption of the renewed node key with at least either a node key

or leaf key on a lower stage of the tree structure to an information player at a leaf where the node key has to be renewed; and

the renewing step further including the steps of:

acquiring a renewed node key by encryption of the key renewal block (KRB); and

calculating renewal data for the generation-managed decryption key based on the thus-acquired renewed node key.

88. The method according to claim 85, wherein:

the generation-managed decryption key has a generation number as renewal information correlated therewith; and

the decrypting step further includes the step of:

reading a generation number of the generation-managed encryption key having been used for encrypting the data from the recording medium; and

decrypting the encrypted data read from the recording medium with a generation-managed decryption key corresponding to the thus-read generation number.

89. An information recording medium to which information can be recorded, the medium having stored therein:

prerecording generation information as generation information on a key allowed as an encryption key usable for writing encrypted data to the information recording medium or a decryption key usable for decrypting data read from the information recording medium.

90. The information recording medium according to claim 89, wherein the prerecording generation information is recorded in an unrewritable area of the information recording medium.

91. A key renewing terminal for serving a renewed generation-managed key to an information recorder or player having a cryptography means for encrypting information to be recorded to a recording medium or an information recorder or player having a cryptography means for decrypting information read from a recording medium, each by a cryptography with a generation-managed key which can be renewed to a different key for each generation, the apparatus comprising:

an interface connectable to the information recorder or player;

means for communications with outside; and

means for controlling each of acquisition of a device-unique identifier from the information recorder or player via the interface, transmission of the device-unique identifier via the communications means, and transfer of the renewed generation-managed key to the information recorder or player via the interface.

92. A key renewing terminal for serving a renewed generation-managed key to an information recorder or player having a cryptography means for encrypting information to be recorded to a recording medium or an information recorder or player having a cryptography means for decrypting information read from a recording medium, each by a cryptography with a generation-managed key which can be renewed to a different key for each generation, the apparatus comprising:

an interface connectable to the information recorder or player;

a storage means having stored therein a key table in which a generation-managed key encrypted with a device-unique encryption key is correlated with an identifier unique to the information recorder or player; and

means for controlling each of acquisition of the device-unique identifier from the information recorder or player via the interface, acquisition, based on the device-unique identifier, of an encrypted generation-managed key corresponding to the device-unique identifier from the storage means, and transfer of the renewed generation-managed key to the information recorder or player via the interface.

93. The medium according to claim 92, wherein:

a mutual authentication is effected with the information recorder or player; and

the generation-managed key is served to the information recorder or player only when the mutual authentication has successfully be made.

94. A generation-managed key renewing method for serving a renewed generation-managed key to an information recorder or player having a cryptography means for encrypting information to be recorded to a recording medium or an information recorder or player having a cryptography means for decrypting information read from a recording medium, each by a cryptography with a generation-managed key which can be renewed to a different key for each generation, the method comprising the steps of:

connecting a key renewing terminal including an interface connectable to the

information recorder or player and means for communications with outside to the information recorder or player;

acquiring a device-unique identifier from the information recorder or player via the interface;

transmitting the device-unique identifier via the communications means;

receiving the renewed generation-managed key via the communications means; and

transferring the renewed generation-managed key to the information recorder or player via the interface.

95. A generation-managed key renewing method for serving a renewed generation-managed key to an information recorder or player having a cryptography means for encrypting information to be recorded to a recording medium or an information recorder or player having a cryptography means for decrypting information read from a recording medium, each by a cryptography with a generation-managed key which can be renewed to a different key for each generation, the method comprising the steps of:

connecting a key renewing terminal including an interface connectable to the information recorder or player and a storage means having stored therein a key table in which a generation-managed key encrypted with an encryption key unique to a device-unique key is correlated with a device-unique identifier of the information recorder or player to the information recorder or player;

acquiring the device-unique identifier from the information recorder or player via the interface;

acquiring, based on the device-unique identifier, an encrypted generation-managed key corresponding to the device-unique key from the storage means; and

transferring a renewed generation-managed key to the information recorder or player via the interface.

96. The method according to claim 95, wherein:

a mutual authentication is effected with the information recorder or player; and

the renewed generation-managed key is served to the information recorder or player only when the mutual authentication has successfully be made.

97. A program serving medium for serving a computer program under which information is recorded to a recording medium in a computer system, the computer program comprising the steps of:

making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of an information recorder and prerecording generation information which is recording-medium generation information prestored in the recording medium;

encrypting information to be stored into the recording medium by a cryptography with a generation-managed encryption key which can be renewed to a different key for each generation; and

effecting at least either outputting of a warning or acquisition of a generation-

managed encryption key of a generation as young as or younger than that indicated by the generation information on the device-stored generation-managed encryption key when the comparison result is that the prerecording generation information is newer than the generation information on the device-stored generation-managed encryption key.

98. The medium according to claim 97, wherein the computer program further including the step of

renewing the generation-managed encryption key by encryption of encrypted data read from the recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information recorders each as a leaf or a leaf key unique to each of the information recorders.

99. A program serving medium for serving a computer program under which information is recorded to a recording medium in a computer system, the computer program comprising the steps of:

making a comparison between generation information on a device-stored generation-managed encryption key stored in a storage means of an information player and recording generation information which is generation information having been used for recording the information to the recording medium;

decrypting information read from the recording medium by a cryptography with a generation-managed decryption key which can be renewed to a different key for each

generation; and

effecting at least either outputting of a warning or acquisition of a generation-managed encryption key of a generation as young as or younger than that indicated by the generation information on the device-stored generation-managed decryption key when the comparison result is that the recording generation information is newer than the generation information on the device-stored generation-managed decryption key.

100. The medium according to claim 99, wherein the computer program further including the step of

renewing the generation-managed decryption key by decryption of encrypted data read from the recording medium with at least either a node key unique to each of nodes included in a hierarchical tree structure including a plurality of different information players each as a leaf or a leaf key unique to each of the information players.